

Amendments to the Claims:

This listing of claims will replace all prior versions of claims in the application:

1. (canceled)
2. (canceled)
3. (canceled)
4. (canceled)
5. (canceled)

6. (currently amended) The portable device as recited in Claim 1 A unitary portable biometrics-based access control device which can be directly plugged into a universal serial bus (USB) socket communicatively coupled to a restricted resource, the device comprising:
a housing;
a microprocessor housed within the housing;
a non-volatile memory coupled to the microprocessor and capable of storing user data
and having a minimum of 8 MB of capacity;
a USB plug integrated into the housing without an intervening cable and capable of
coupling the unitary portable access control device directly to the USB socket;
and
a biometrics-based authentication module coupled to and controlled by the
microprocessor, at least a portion of the biometrics-based authentication module
being housed within the housing, wherein said biometrics-based authentication

module is configured to grant access to the restricted resource provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the restricted resource is denied to the user otherwise; and further wherein

said biometrics-based authentication module is configured to grant access to the user data stored in the non-volatile memory provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the user data stored in the non-volatile memory is denied to the user otherwise,

wherein the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.

7. (canceled)
8. (canceled)
9. (canceled)
10. (canceled)
11. (canceled)
12. (canceled)
13. (canceled)
14. (canceled)
15. (canceled)

16. (currently amended) The biometrics based access control system as recited in Claim 11
A biometrics-based access control system for controlling access to a restricted resource,
comprising:

a portable device which can be directly plugged into a universal serial bus (USB) socket
communicatively coupled to the restricted resource and which includes
a housing;

a non-volatile memory housed within the housing and having a minimum of 8
MB of capacity;

a USB plug integrated into the housing without an intervening cable and capable
of coupling the portable device directly to the USB socket; and

a biometrics-based authentication module coupled to the non-volatile memory,
wherein the biometrics-based authentication module is configured to (1) capture a first
biometrics marker, (2) store the first biometrics marker in the non-volatile
memory; (3) capture a second biometrics marker; and (4) determine whether the
second biometrics marker can be authenticated against the first biometrics marker,
and wherein access to the restricted resource is granted upon a determination of
successful authentication and wherein access to the restricted resource is denied
otherwise.

wherein a bypass mechanism for authentication is provided upon a determination of
authentication failure by the biometrics-based authentication module.

17. (canceled)

18. (canceled)

19. (canceled)
20. (canceled)

21. (currently amended) The biometrics-based access control method as recited in Claim 17
A biometrics-based access control method for controlling access to a restricted resource
and implemented using a portable device, the method comprising the steps of:
 - (a) directly plugging the portable device into a universal serial bus (USB) socket
communicatively coupled to the restricted resource, wherein the portable device
includes a housing; a memory having a minimum of 8 MB of capacity; a
biometrics sensor; and a USB plug integrated into the housing without an
intervening cable and capable of coupling the portable device directly to the USB
socket;
 - (b) obtaining a first biometrics marker from a user with the biometrics sensor of the
portable device;
 - (c) retrieving a registered biometrics marker from the memory of the portable device,
the registered biometrics marker having been stored therein during a registration
process;
 - (d) comparing the first biometrics marker against the registered biometrics marker;
and
 - (e) granting the user access to the restricted resource provided that a match is
identified in said step (d), and
further comprising the step of providing the user with a bypass authentication procedure
provided that a match is not identified in said step (d).

22. (canceled)

23. (canceled)

24. (canceled)

25. (canceled)

26. (canceled)

27. (canceled)